***** PUBLIC VERSION *****

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE EASTERN DISTRICT OF VIRGINIA**
**Alexandria Division**

| | |
|---|---|
| UNITED STATES OF AMERICA,<br>Plaintiff,<br>v.<br>ZACKARY ELLIS SANDERS,<br>Defendant. | Case No. 1:20-cr-00143<br>Honorable T.S. Ellis, III<br>Sentencing: April 1, 2022 |

**MEMORANDUM IN SUPPORT OF MOTION FOR NEW TRIAL AND TO RECONSIDER MOTIONS TO COMPEL AND MOTIONS TO SUPPRESS**

The defense understands and respects the Court's prior rulings on Mr. Sanders's Motions to Compel and Motions to Suppress. To ensure a complete appellate record and to make the Court aware of recently discovered information relevant to its prior rulings, however, the defense now submits significant additional materials it has obtained through its own investigation since the Court's resolution of Mr. Sanders's most recent motions to compel and suppress.

In light of these additional materials, and as discussed below, Mr. Sanders respectfully moves the Court to order a new trial in this case under Federal Rule of Criminal Procedure 33. Mr. Sanders further respectfully moves the Court to grant Mr. Sanders's previously filed Motions to Compel, order a hearing pursuant to *Franks v. Delaware,* 438 U.S. 154 (1978), and suppress all evidence obtained pursuant to the invalid search warrant because it was not supported by probable cause and was based on an affidavit containing numerous and material false and misleading statements and omissions.[1]

[1] Under Rule 33, "the court may vacate any judgment and grant a new trial if the interest of justice so requires." Fed. R. Crim. P 33(a). "A motion for a new trial grounded on newly

The newly discovered materials warrant a new trial, the production of additional material from the government, and suppression for at least the following seven reasons. First, the materials reveal for the first time that the Foreign Law Enforcement Agency (FLA) that seized the Target Website ([redacted] in June 2019 was not the [redacted] ([redacted] but some undisclosed country.[2] Among other implications of this disclosure—which was made by federal prosecutors to a defendant in a separate case arising from the same operation—is that the Affidavit misled the Magistrate Judge by, *inter alia* and at the very least, using the term "FLA" to refer to multiple countries, and not just the [redacted] Critically, nowhere did the Affidavit provide assurances that *the unknown FLA that seized Mr. Sanders's IP address* (1) "obtained that IP address information through independent investigation" not involving the U.S.; (2) had conducted an investigation that "was lawfully authorized in the FLA's country pursuant to its national laws;" (3) was from "a country with an established rule of law;" (4) had a long history of exchanging "criminal investigative information with U.S. law enforcement, across disciplines and including the investigation of crimes against

---

discovered evidence must be filed within 3 years after the verdict." Fed. R. Crim. P. 33(b)(1). With respect to the additional relief requested, this motion renews and supplements Mr. Sanders's Motions to Compel (ECF No. 38, 255, 137, 335), Motion to Suppress Due to Lack of Probable Cause (Motion to Suppress No. 1) (ECF No. 81-82), Motion to Suppress Based on False and Misleading Material Information in Affidavit Paragraph 23 (Motion to Suppress No. 2) (ECF No. 85-86), Motion to Suppress Based on Materially Misleading Statements and Omissions Regarding Tor, the Target Website, and the Subject Premises (Motion to Suppress No. 3) (ECF No. 83-84), and Motion to Suppress Based on False and Misleading Material Information in Affidavit Paragraph 25 (Motion to Suppress No. 4) (ECF No. 90-91). Mr. Sanders also incorporates by reference the following prior pleadings and related exhibits: ECF No. 48, 58, 93, 109, 112, 140, 176, 241, 252, 253, 256, 354, 427, 467, 476, and 491.

[2] The unnamed FLA is known to the government but not to the defense. *See Kiejzo* Transcript, attached as Ex. 1, at 20 (government stating that it knows the identity of the FLA that seized the target website).

children;" and (5) "had not interfered with, accessed, searched, or seized any data from any computer in the United States in order to obtain that IP address information." Affidavit (ECF No. 254-3) ¶ 25. In fact, contrary to a plain reading of the Affidavit, it contains no representations regarding the reliability of the country (or law enforcement agency) that took control of the website and then deployed the method used to seize Mr. Sanders's IP address.

The government has not disclosed what country (and what law enforcement agency within that country) deployed the method that was used to obtain the IP address information that the [redacted] ultimately provided to the FBI in August 2019. That is true even though the reliability of that country and law enforcement agency, as well as the method it deployed, are essential to the probable cause determination. A double-hearsay tip from an unknown country—without any representation about the reliability of the method used to obtain the information or a track record of reliable intelligence from that country—cannot possibly support probable cause.

Second, these materials further demonstrate that the FBI understood (or should have) that the tip meant only that the Sanders family's IP address was used on a single occasion to access, *i.e.* visit, a single website that included links to, *inter alia*, child pornography.[3] Based upon the twelve other cases the defense has now obtained (and which were not available to the defense at the time the earlier motions to compel and motions to suppress were filed) involving the same

[3] These links were available only to a registered, logged-in user, and the FBI had no evidence that someone using the Sanders family's IP address ever went past the homepage, registered an account, logged in, or clicked on any child pornography on the target website, all of which were prerequisite steps to viewing illegal content. *See also United States v. Vincent Kiejzo*, Case No. 20-cr-40036-TSH (D. Mass., Oct. 19, 2021) (ECF No. 117 at 3) ("*Kiejzo* Transcript") at 41, attached as Ex. 1 (government counsel acknowledging that "access[ing]" the website and "logg[ing] in" to the website were not equivalent, that "[t]he United States is not in possession of . . . information . . . that [the defendant in *Kiejzo*] in particular created an account," and that "[t]he only information [the U.S.] was provided was that the IP address that was linked to his house accessed these websites"); *see also id.* at 43 (similar).

FLA tip, law enforcement's understanding of the tip's true meaning with respect to the Sanders family's IP address is plain: that the IP address was used just once to access (*i.e.*, visit) *a website*, and not any particular content. *See, e.g.,* Case Comparison, attached as Ex. 20, at 1-5.

Moreover, there is a clear pattern reflected in the other cases, relevant to the probable cause determination, of law enforcement not seeking a search warrant where there was nothing other than a bare tip. As set forth *infra* at 12-14, in the other cases arising from the same operation, law enforcement had additional "derogatory" information regarding the suspect, such as corroboration of the suspect's interest in child pornography, previous convictions, voluntary interviews with the suspect involving inculpatory information, and incriminating information collected pursuant to pen register/trap and trace warrants. Indeed, of the twelve cases obtained by the defense and discussed below, only here did law enforcement obtain a search warrant based on the bare tip alone. Ex. 20 (Case Comparison) at 6-8. This pattern demonstrates that even law enforcement believed that more was required for probable cause than the bare FLA tip. Indeed, the government itself has expressly recognized that the information reflected in the FLA tip is insufficient for probable cause.[4]

[4] In *United States v. Nikolai Bosyk*, 17-CR-302 (E.D. Va. 2018), the government, in opposing the defense's motion to suppress, reasoned that "[w]hile merely joining an e-group [on Tor] without evidence that an individual either attempted to or did acquire illicit material falls short of the Fourth Amendment's requirements"—because "merely joining an e-group is not illegal"—"a click of a URL, that was advertising child pornography on a website dedicated to child pornography, does establish probable cause." Defense Ex. (ECF No. 109-A) at 11-12. Here, there was no evidence that the IP address was ever used to register an account on [redacted] let alone click on a post that advertised or contained illegal content. *Compare* 2020/07/31 Tr. (ECF No. 255-1) at 33 ("MR. CLAYMAN: . . . the face of the tip . . . says they did go in, they did access illegal content) *with* 2020/09/11 Tr. (ECF No. 137-1) at 25 ("MR. CLAYMAN: . . . Admittedly, we don't know precisely what the content is, but we have never claimed to know exactly what it is, or exactly the definition of child pornography under the United States Code. We also never claimed that the tip alleges that he downloaded that content."). *See also* Ex. 2 (*Kiejzo* Objection) at 18 (The government represented in *Kiejzo* that "it is not in possession of information showing which portions of Websites 2 and 3 the IP address accessed."); *compare*

Third, these materials reveal that U.S. law enforcement had access to a searchable copy of [redacted] as early as January 2020 (and likely much earlier) and continued to even after the site was purportedly shut down. The government previously dismissed as "speculative . . . that additional information related to . . . the FLA's tip might exist." ECF No. 43 at 6. In possession of a copy of [redacted] all along, however, the FBI had the ability to search for evidence regarding Mr. Sanders's alleged activity on the website (or lack thereof) by, for example, correlating the precise time the FLA said Mr. Sanders allegedly visited the site (02:06:48 UTC) with [redacted] server logs. This shows that the government had access to much more information regarding Mr. Sanders activity on the site (or lack thereof) than it has previously acknowledged—information it should have produced to the defense. Furthermore, to the extent the government claims it could not access this information because it did not have Mr. Sanders's username, that claim only underscores that the government has known all along that the FLA tip meant that Mr. Sanders's merely "accessed" the site, and not any content available only to a registered, logged-in user.

Fourth, the newly discovered materials further demonstrate that this case arose from an operation that was massive in scope and involved hundreds if not thousands of IP addresses. Those IP addresses were obtained after an undisclosed country took over the website. The operation was so large that, as in Operation Pacifier, a.k.a., "Playpen," the FBI used boiler-plate affidavits and FD-1057s that required only minor modifications, *see infra* at 18-22, which is further evidence that the investigation involved a Network Investigative Technique ("NIT"), a technique that necessarily interferes with computers wherever they are located. *See also*

---

*with* 2019/12/09 1057, attached as Ex. 3 (providing that the FBI had evidence that a user had logged onto [redacted] not just accessed [redacted]

Murdoch Decl. (ECF No. 467-2) at ¶ 31 ("Traffic analysis is extremely unlikely to yield the hundreds of IP addresses submitted by the [redacted] ([redacted] nor give the [redacted] confidence that these IP addresses visited the Onion Service in question"). That calls into serious question the government's representations in the Affidavit that no U.S. computer was interfered with.

Fifth, newly discovered material from a case arising from the same investigation demonstrates that the Affidavit was additionally misleading regarding the meaning of the tip and the probability of whether a single visit to the target website would have been followed by additional visits. By phrasing statistical information about users' prior conduct in a way that did not accurately portray the statistics gleaned from a prior operation (Operation Pacifier and the Playpen website), the tip falsely suggested indicia for probable cause that did not exist.

Sixth, the materials demonstrate that U.S. law enforcement was working more closely with foreign law enforcement agencies than was previously acknowledged. An FBI document demonstrates conclusively that the FBI opened its preliminary investigation into [redacted] in January 2017, more than two years before the IP addresses that had purportedly visited [redacted] were identified by a foreign law enforcement agency and transmitted to the FBI. In an affidavit that arose from the same operation as this case, law enforcement described the investigation as "collaborative" between U.S. and foreign law enforcement. *United States v. Thomas S. Clark*, Case No. 2:21-MJ-00147-JLW (W.D. Wash., March 11, 2021) (Complaint) ("*Clark* Complaint") attached as Ex. 4, at ¶ 5. Recent press releases and the volume of information that the FBI obtained in reference to this investigation are additional evidence that this was a joint operation labeled "Operation H," where U.S. law enforcement were working hand in hand with foreign law enforcement agencies to share information, take over targeted websites, and identify visitors to

those websites. *See infra* at 25-29; *compare with* ECF No. 476-2 (previous press releases noting that the [redacted] and other international law enforcement partners, through work with FBI LEGATs, were crucial to taking down Tor websites); *see* also ECF No. 138-6 (showing [redacted] and US law enforcement as having led the takedown of a Tor website, along with other "international partners").

Finally, and relatedly, the recent disclosures demonstrate that there is a significant amount of withheld discovery material to Mr. Sanders's suppression issues. This material includes, but is not limited to, the identity of the country (and agency) that infiltrated the website, the identity of the country (and agency) that deployed a technique that identified Mr. Sanders's IP address (and the circumstances of that identification); and the user history and logs from [redacted] which the FBI has now expressly admitted in *United States v. Zachary M. Stauffer*, Case No. 4:20-MJ-04005-RJD (S.D. Ill., Jan. 28, 2020) (Complaint) ("*Stauffer* Complaint), attached as Ex. 5, as in its control and/or possession. This material should have been produced in order for the suppression issues to have been decided on a fair and accurate record. This material should now be produced, at minimum to the Court for *in camera* inspection.

## DISCUSSION

### I. The government's recent disclosure that the [redacted] was not the law enforcement agency that seized the target website undermines the government and law enforcement's representations on the paramount issue of the tip's reliability.

Based on a disclosure by federal prosecutors to the defense in a separate case from the same operation, it is now clear that there was a third country involved in the investigation of the target website whose rule of law and reliability are not addressed in the Affidavit. *See* Ex. 2

(*Kiejzo* Objection) at 2, 6-7; *see also* Ex. 1 (*Kiejzo* Transcript) at 8.[5] Given that disclosure, and the ensuing likelihood that it was this undisclosed FLA that deployed the technique that seized Mr. Sanders's IP address, Paragraph 25 of the Affidavit painted a false picture to the Magistrate Judge. It did so by providing assurances regarding the tip's integrity and reliability that would only have mattered were it the [redacted] that had initially identified Mr. Sanders's IP address (rather than merely providing that information second-hand to the FBI). Indeed, the Affidavit strongly suggests that only one FLA was involved by repeatedly referencing "*a*" FLA or "*the*" FLA, without ever providing that those references were (or could have been) discussing different agencies from different countries. *See* Affidavit (ECF No. 254-3) at ¶ 15 ("In June of 2019, the computer server hosting the TARGET WEBSITE, which was located outside of the United States, was seized by a foreign law enforcement agency."); *see also id.* at ¶¶ 23-26, 31 (referring to "a foreign law enforcement agency" as the "FLA" and emphasizing the long history of the U.S. sharing information with the FLA, and the FLA sharing information with the U.S., and the reliability in the past of tips from the FLA). The government reinforced this impression to the defense and the Court. *See, e.g.*, 2020/09/11 Tr. (ECF No. 137-1) at 23-24 ("As Your Honor knows from having reviewed the tip and the affidavit, the tip came from a well-respected foreign law enforcement agency," but failing to mention the role of a second FLA).

The *Kiejzo* case arose from the same law enforcement operation as this case.[6] In *Kiejzo*, an agent from the Department of Homeland Security's Homeland Security Investigations (HSI)

[5] This transcript of proceedings that took place on Oct. 12, 2021, was released to the public on January 10, 2022.

[6] *Cf. United States v. Paul Bateman*, Case No. 1:20-cr-10012-IT (D. Mass, Dec. 27, 2021) (ECF No. 106 at 2-3, n.3) ("*Bateman* Motion") ("The government in the instant case confirmed that both the instant case and *Kiejzo* arose out of the same investigation, and also confirmed . . . that there was another, separate FLA local to the server host country that conducted the seizure of

agency submitted an affidavit alleging that "in August 2019, an FLA notified U.S. law enforcement that a specific IP address was twice 'used to access online child sexual abuse and exploitation material via … website[s] that the FLA named and described as Website[s] 2 [and 3]' on a specific date in May 2019." Ex. 2 (*Kiejzo* Objection) at 2 (quoting from affidavit). The transcript from the motions hearing in *Kiejzo* shows that, unlike here, the government, in compliance with its *Brady* obligations, disclosed to defense counsel "that the foreign law enforcement agency who seized the server back in June, 2019 was *not* the foreign law enforcement agency that provided the tip and *did not even originate from the same country* that the government has assured us is bound by the rule of law, the same rule of law that it relies upon to justify the warrant." Ex. 1 (*Kiejzo* Transcript) at 8 (emphasis added). At the October 12, 2021 motions hearing, the government represented to the court that "the United States *does know* the name of this foreign law enforcement agency that was seizing" the target website. *Id.* at 20 (emphasis added).[7] It appears that this information, as in this case, was not presented in the affidavit that law enforcement submitted in support of the search warrant.

The FLA that seized the website would naturally be the same FLA that deployed the technique identifying visitors to the website. Indeed, in at least one other case from the same operation, law enforcement confirmed this understanding. *See United States v. Brent M.*

---

Website A's server – an FLA distinct from the tip-providing FLA referenced throughout [the HSI agent's] affidavit.") (attached as Ex. 6).

[7] Prior to that hearing, the government informed Mr. Kiejzo's counsel that the server for the website was located outside of the United States and outside the FLA's country, and that the foreign law enforcement agency that seized the server was local to that host country, but neither the FBI nor the HSI *agents* knew which country the server had been located in. *United States v. Vincent Kiejzo*, Case No. 20-cr-40036-TSH (D. Mass., Oct. 19, 2021) (ECF No. 117 at 3) ("*Kiejzo* Objection"), attached as Ex. 2.

*Lawson*, Case No. 4:21-CR-00155-MTS (E.D. Mo., Dec. 17, 2021) (Guilty Plea Agreement) ("*Lawson* Plea Agreement"), attached as Ex. 7 at 4 ("Law enforcement infiltrated this dark web website [referring to [redacted] and determined that the defendant had utilized the website."); *see also* Murdoch Decl. (ECF No. 467-2) at ¶¶ 22-28 (explaining that "[i]n order to use an NIT, law-enforcement must control the Onion Service prior to deploying the NIT"); *see id*. at ¶ 32 (concluding that "law-enforcement almost certainly controlled the Onion Service [[redacted] prior to May 23, 2019 [the date that the Sanders family's IP address was alleged to have visited the site]"). The government's apparent claims to the contrary are not accurate. *See, e.g.,* 2020/03/04 Government Email, attached as Ex. 8, at 1 ("The information in the search warrant that [Mr. Sanders's] IP address accessed child sexual abuse material in May 2019, prior to the seizure of the computer server, came from the [redacted] and the [redacted] collected this data through its own independent investigation using lawful investigation techniques").

*Kiejzo* establishes that there was a third country involved in the investigation of the target website and that this country shared information with the [redacted] and/or the U.S. This kind of double-hearsay, standing alone and without any indicia of reliability about the method used by the third country or the third country itself, cannot be sufficient for probable cause.

The prosecutors here—unlike the prosecutors in *Kiejzo*—failed to disclose the third country's role in seizing the website and identifying Mr. Sanders's IP address. That remained the case even while the prosecutors knew that the defense (and the Court) was acting under the reasonable belief that the FLA referred to in the Affidavit and the seizing FLA were one and the same. *See, e.g.,* Defense Suppl. Brief (ECF No. 58) at 8, n.7 (failing to correct the defense after the defense stated that at some point the [redacted] would have communicated to the FBI "that the [redacted] seized [redacted] in June 2019"); Memorandum in Support of Motion to Suppress No. 2

(ECF No. 253) at 12 (failing to correct the defense after the defense stated that "[t]he FBI captured numerous screenshots of [redacted] in January 2019, six months before the [redacted] seized and shut down the website in June 2019"); Motion to Compel (ECF No. 137) at 16 (failing to correct the defense after the defense stated that the screenshot of the target website's homepage was uniquely in the government's possession, "given that the [redacted] shut down the website in June 2019"); Memorandum Op. (ECF No. 73) at 3-4, 6, 12-13 (relying on the belief that the [redacted] identified the IP addresses, that the [redacted] in identifying the IP addresses—asserted that it had not interfered with a computer in the United States, and that "foreign law enforcement agency" referenced in the affidavit referred only to the [redacted] [redacted] Sealed Order (ECF No. 107) at 1 (reflecting the understanding that the information comprising the tip originated from the [redacted] [redacted] not another law enforcement agency or third country); Sealed Memorandum Op. (ECF No. 113) at 1-4 (reflecting the understanding that the foreign law enforcement agency described in the affidavit was the [redacted] [redacted] *id.* at 8 (concluding there is no doubt that a "presumption of credibility extends to reliable foreign law enforcement agencies like the FLA in this case, the [redacted] [redacted] Sealed Order (ECF No. 236) at 6 (emphasizing the importance of the FLA's reliability as to why the affiant was warranted in relying on the FLA tip).

Based on the above, and when the Affidavit is understood in light of the *Kiejzo* disclosure, the tip no longer has any indicia of reliability. The Court should accordingly grant Mr. Sanders a new trial and suppress the physical evidence derived from the search warrant in this case. In the alternative, the Court should order the government to disclose the identity of the seizing FLA in this case and all materials reflecting its role in the seizure of the target website and the identification of Mr. Sanders's IP address.

## II. The FBI understood the true meaning of the FLA's tip and that the tip, by itself, was insufficient to establish probable cause.

Materials recently obtained from other cases that arose from the same law enforcement operation further corroborate the defense's arguments that the FBI understood (or should have) that (1) the FLA's tip meant only that the Sanders family's IP address was used on a single occasion to visit a single website—not to view or download child pornography from a website; and (2) a bare FLA tip involving a single visit to a target website, without further evidence that a resident of the subject premises had an interest in child pornography or previous criminal history, was insufficient for probable cause.

Since the defense filed its most recent renewed motions to compel and to suppress, it has received additional information pertaining to twelve other cases[8] that involved substantially the same FLA tip present in this case and which arose from the same operation. Ex. 20 (Cases Stemming from Same Operation) at 1-5.

In *all* of those twelve cases except the instant one (and possibly in *Bateman*, a case in which the search warrant affidavit remains under seal), law enforcement did not rely exclusively upon the FLA tip that an Internet user had visited a target website on one occasion to obtain a search warrant. *Id.* at 6-8. To the contrary, law enforcement sought search warrants only where it had the same tip (or a more derogatory tip) plus other incriminating evidence. *Id.* at 6-8. The most reasonable inference to draw from the related cases is that law enforcement knew that an FLA tip providing that an IP address accessed the homepage of [redacted] at a single point in time is not sufficient evidence for probable cause.

[8] Previously, the defense was only aware of three of these twelve cases as stemming from the same operation. Nine of the twelve cases were unknown to the defense prior to this pleading.

In three cases, the FBI relied on additional information obtained from an FLA for probable cause because the FLA offered evidence that someone using a particular IP address had accessed multiple targeted sites or accessed a single targeted site on numerous occasions. *See, e.g., In the Matter of the Search of Property of 5855 Hunting Lodge Road, Pleasant Garden, NC 27313*, Case No. 1:20-MJ-243-LPA (M.D.N.C., Aug. 18, 2020) (Affidavit in Support of Search Warrant) ("North Carolina Affidavit"), attached as Ex. 9, at ¶¶ 54-55 (IP address was alleged to have visited three target websites); *In the Matter of the Search of 54 Spruce St., Apartment 6, Burlington, VT*, Case. No. 2:20-MJ-00143-KJD (D. Vt., Dec. 4, 2020) (Affidavit in Support of Search Warrant) ("Vermont Affidavit"), attached as Ex. 10, at ¶ 36 (IP address was alleged to have visited the target website on six dates and times); Ex. 2 (*Kiejzo* Objection) at 11 (IP address was alleged to have accessed two target websites on same date).

In five other cases where information from the FLA was similar to the information provided in Mr. Sanders's case (*i.e.*, accessing the website at a single point in time), law enforcement relied on additional derogatory information, including the fact that residents of the subject premises had prior criminal records for sex offenses, thereby corroborating the tip. *See, e.g.,* Ex. 5 (*Stauffer* Complaint) at ¶ 8 (resident was a convicted sex offender); *In the Matter of Search of Premises located at 6603 Crimson Lane, Barnhart Missouri, 63012*, Case No. 4:20-MJ-3301-NCC (E.D. Mo., Nov. 12, 2020) (Affidavit in Support of Search Warrant) ("Missouri Affidavit"), attached as Ex. 11, at ¶ 38 (same); Ex. 4 (*Clark* Complaint) at ¶ 14-15 (same); *In the Matter of the Search of 4068 Fairbanks Drive, Chipley, Florida 32428*, Case No. 5:20-MJ-44-MJF (N.D. Fl., May 6, 2020) (Affidavit in Support of Search Warrant) ("Florida Affidavit"), attached as Ex. 12, at ¶¶ 41-42 (prior arrest and pending charge for sexual abuse of children); *In the Matter of the Search of Entire property located at 291 Old Brunswick Rd., Gardiner, Maine*

*04345*, Case No. 1:20-MJ-00255-JCN (D. Me., Sept. 8, 2020) (Affidavit in Support of Search Warrant) ("Maine Affidavit"), attached as Ex. 13, at ¶ 30 (resident was previously arrested for public indecency).

The remaining three cases are particularly telling. In those cases — where residents did not have prior criminal records and where (like here) the information provided by the FLA was only that an IP address accessed the website at a single point in time —law enforcement did not initially seek search warrants at all, instead opting first for investigatory methods that did not require a showing of probable cause. In two cases, law enforcement tried "knock and talks" first. *See, e.g.,* Ex. 5 (*Stauffer* Complaint) at ¶¶ 11, 14 (two voluntary interviews and one consensual search of devices); *Corwin* Complaint (ECF No. 354-9) at ¶¶ 5-9; *In the Matter of the Search of the premises known as 31 Adams Avenue, Rochester, NH,* Case No. 1:21-MJ-00146-AJ (D. NH., June 7, 2021) (Affidavit in Support of Search Warrant) ("New Hampshire Affidavit"), attached as Ex. 14, at ¶¶ 9-15, 17-24 (one voluntary interview with husband and one with wife). And in the remaining case, law enforcement first sought a pen register/trap and trace warrant to attempt to corroborate the tip. *In the Matter of Search at 234 South Magnolia Avenue, Lansing Michigan 48912*, Case No. 1:20-MJ-00481-SJB (W.D. Mi., Nov. 19, 2020) (Affidavit in Support of Search Warrant) ("Michigan Affidavit"), attached as Ex. 15, at ¶ 32 (law enforcement corroborated that Internet user repeatedly connected to Tor).

Only in Mr. Sanders's case did law enforcement submit it had probable cause based on nothing more than an FLA tip reflecting a single visit to a single target website. This provides yet another basis for the Court to conclude that the search warrant in this case was not supported by probable cause. Based thereon, the Court should grant Mr. Sanders a new trial and suppress the physical evidence obtained from the invalid warrant.

**III. The FBI has had access to a copy of the target website all along, undermining the government and law enforcement's representations about Mr. Sanders's purported accessing of content on the site and on the FBI's level of cooperation with the FLA.**

Based upon the newly discovered evidence, it is now clear that at some point the FBI either seized [redacted] itself (and possibly ran the website) or otherwise obtained a forensic copy. In *Stauffer*, the FBI noted its ability, in January 2020, to look up the online activity related to users of [redacted] even though [redacted] had purportedly been seized and shut down back in June 2019. On January 7, 2020, agents went to Mr. Stauffer's home and talked to him. He "admitted to downloading TOR on his desktop computer in his house . . . and accessing websites to view pictures and videos of child pornography," including "websites such as [redacted] Ex. 5 (*Stauffer* Complaint) at ¶¶ 10-11. He told the agents that he "visited [redacted] multiple times a week, from at least one year ago until [redacted] was shut down," and that his account on [redacted] was "'kittycow' with a password of 'thundercat.'" *Id.* at ¶ 11. *Just three days later*, on January 10, 2020, the FBI Child Exploitation Operations Unit provided information about "the online activity of the username 'kittycow' and 'kittycow2," and a sample of messages posted by the user 'kittycow2'." *Id*. at ¶ 13.

The FBI's ability to search [redacted] in January 2020 (and likely much earlier) is significant for at least two reasons. First, it undermines the representation in Paragraph 25 of the Affidavit that the FLA's investigation of [redacted] was independent from the FBI's; given that the FBI has had a searchable copy of the site for years, its role in the investigation of [redacted] was clearly more significant than it has disclosed, thus undermining the representation in Paragraph 25 of the Affidavit that the FLA (or FLAs) investigations were "independent." Affidavit ¶ 25. Second, it shows that the FBI had much more information regarding Mr. Sanders than it has admitted. Given that it has been in possession of a searchable copy of the website all

along, it had the ability to search using the tip information, *i.e.*, the exact second Mr. Sanders is alleged to have accessed the site (02:06:48 UTC), to examine Mr. Sanders activity (or lack thereof) on the website. The FBI would therefore have been in possession of additional exculpatory information that it did not disclose to the Magistrate Judge and has not disclosed here, including evidence that Mr. Sanders's IP address was not used to register for the site, view child pornography, or download or post any material on the site.[9]

The government has informed the defense that it required a username—which it does not have for Mr. Sanders—in order to investigate Mr. Sanders's activity on the FBI's copy of the site. In an email to the defense on March 3, 2022, the government stated that it "cannot investigate [Mr. Sanders's] activity on the Target Website beyond what was described in the search warrant affidavit because we do not know his username." Ex. 8 (2022/03/04 Government Email) at 3. While that still does not address the issue of searching based on the pinpointed access time (02:06:48 UTC) raised above, it also raises an even more troubling issue. The government is stating that it could review Mr. Sanders's activity on the website *only if* it had a username for Mr. Sanders, which it does not. And yet the Affidavit submitted to the Magistrate Judge plainly stated that the IP user "accessed child exploitation and sexual abuse material via a website." Affidavit (ECF No. 254-3) at ¶ 23. If the government knew that it was not possible to ascertain user activity on the website in the absence of a username, then it also knew that Paragraph 23's assertion that the IP user accessed *content* on the website was false, as were its similar representations to this Court. *See* 2020/07/31 Tr. (ECF No. 255-1) at 33 ("MR.

[9] Both the [redacted], and the FD-1057 (ECF No. 427-5B) are inconsistent with the government's continued claim that the tip meant that the Sanders family's IP address viewed any illegal content on [redacted] as opposed to merely visited [redacted] one time.

CLAYMAN: the face of the tip . . . says [Mr. Sanders] did go in, [he] did access illegal content").

Based on these new disclosures, as well, the Court should grant Mr. Sanders's motion for a new trial and suppress the evidence seized pursuant to the invalid search warrant. In the alternative, the Court should compel the government to produce information in its possession regarding Mr. Sanders's IP address and its activity (or lack thereof) on the site.

## IV. The additional materials demonstrate that this was an international effort that was massive in scope, which contradicts the information presented in the government's affidavit and is additional evidence that an NIT was used to identify those IP addresses.

New materials show that, contrary to the government's representations to the Magistrate Judge, the FBI was involved in an international effort to investigate visitors to Tor websites long before it was provided the tips about [redacted] and other sites, in August 2019. *See United States v. Dashawn* Webster, Case No. 2:18-CR-101-RAJ (E.D. Va., Jan. 30, 2019) (Transcript) ("Webster Sentencing Transcript"), attached as Ex. 16, at 8-10 (HSI agent testifying that "several agencies, international, national had to work together to try to identify [the defendant]" on at least five or six Tor websites that contained child pornography, and that other individuals were also arrested that were connected to the same site(s)). The FBI opened its preliminary investigation into [redacted] in 2017, more than two years before an FLA identified a large number of IP addresses as having visited the site in April and May 2019. *See, e.g.,* 2017/01/13 FD-302, attached as Ex. 17 (documenting preliminary investigation of [redacted] in January 2017, more than two years before IP addresses were identified as having visited [redacted] *see also* 2017/01/13 FD-340, attached as Ex. 18 (documenting collection of [redacted] screenshots that contained obscene material); *compare with* [redacted] News Stories 1-3 (ECF Nos. 476-3 to 476-5). Given that this information contradicts the Affidavit, the government should be ordered

to reveal the FBI's role in investigating [redacted] from 2017 through the identification of and investigation into the Sanders family's IP address.

The additional materials the defense has obtained further reveal the scope of this operation, which could only have arisen from the use of an NIT. As Mr. Sanders has argued in past motions—but which bears repeating here—a foreign law enforcement's use of an NIT in a joint investigation with the FBI violates the Fourth Amendment if, as here, there was no warrant obtained for the deployment of that technique. The government knows this—previously, the FBI had sought a warrant before deploying an NIT, including in Operation Pacifier (a.k.a. "Playpen"). Here, documentation from other cases, as well as materials obtained through Freedom of Information Act releases, suggest that the [redacted] operation followed the same model as Operation Pacifier in terms of having a centralized, structured operation, where "[a]ppropriate draft search warrant affidavits, lead packages, and EC's [(electronic communications), also known as FBI FD-1057s)] have already been written and will be provided" to relevant personnel, and "require only slight modification." Operation Pacifier Process, attached as Ex. 19 at 1. Such efforts to streamline are used precisely because an NIT generates such a large volume of potential leads.

It is clear that, in August 2019, FBI Headquarters understood the significance of this international operation and accordingly immediately launched a bulk, centralized response upon receiving the IP address information as part of that operation, as evidenced by the substantially identical affidavits and electronic communications (also known as EC's or FD-1057's). This is evidence of an investigative scope that only could have been obtained through the deployment of an NIT. Murdoch Decl. (ECF No. 467-2); Clayton Decl. (ECF No. 256-8).

Numerous cases initiated in or after 2019 followed the exact same or similar timelines to this case, because they were all part of the same bulk operation that relied on the same form documents. *See also* ECF No. 476 at 3-9. That timeline supports the inference that IP addresses were obtained using an NIT. As in this case, the tips in other cases were all provided in August 2019, regarding activity that purportedly took place in either April 2019 or May 2019. *See* Ex/ 20 (Cases Stemming from Same Operation); *see also* Ex. 15 (Michigan Affidavit) at ¶¶ 27-28 (noting that in August 2019, as part of the tip, the FLA provided "documentation naming TARGET WEBSITE, which the FLA referred to by its actual name"). In many of those cases, the FBI issued administrative subpoenas to various Internet Service Providers on September 10, 2019.[10] Only after the FBI had issued administrative subpoenas in relation to numerous tips, however, did the FLA provide its September 16, 2019 letter to FBI Supervisory Special Agent Donahue, stating that it had obtained the IP address information it transmitted to the FBI in August 2019 without interfering with any computer in the United States. FLA Letter (ECF No. 253-2). The additional materials attached in support of this memorandum further support that the September 16, 2019 letter was meant to provide a post-hoc justification for the FBI's prior

[10] Sept. 10, 2019 Subpoena (ECF No. 335-1) at 1-2 (administrative subpoena to Cox Communications signed by J. Brooke Donahue on Sept. 5, 2019, pursuant to FBI HQ case, for records relating to the Sanders family's IP address, "98.169.118.39 used on 5/23/2019 at 02:06:48 UTC," and issued on Sept. 10, 2019; Ex. 5 (*Stauffer* Complaint) at ¶ 7 ("On September 10, 2019, the FBI issued an administrative subpoena to Charter Communications."); *United States v. Brandon Kidder*, Case No. 1:21-CR-00118-LJV (W.D.N.Y., Mar. 17, 2020) (Complaint) ("*Kidder* Complaint") (attached as Ex. 21) (same); Ex. 4 (*Clark* Complaint) at ¶ 10 ("On or about September 5, 2019, a summons was issued to Cox Communications."); Ex. 14 (New Hampshire Affidavit) at ¶ 9 ("On or about September 9, 2019, a summons was served on Atlantic Broadband for subscriber information."); *United States v. Michael* Clemence, Case No. 1:21-CR-00099-LM (Affidavit in Support of Criminal Complaint for Michael Clemence) ("*Clemence* Complaint"), attached as Ex. 22, at ¶ 7 (same).

issuance of administrative subpoenas and to conceal the fact that another country deployed an NIT.[11]

After the FBI received information in response to administrative subpoenas, it relayed that information to FBI field offices and HSI offices in the form of lead packages, complete with pre-populated affidavits and draft 1057s. *See, e.g.,* FD-1057 (ECF No. 427-5B) (case opening document for investigation into the Sanders family's IP address after FBI HQ had previously subpoenaed records related to this IP address); Ex. 10 (Vermont Affidavit) at ¶ 49; Ex. 3 (2019/12/09 1057). These lead packages identified IP addresses (and the premises they were linked to) that were suspected of accessing one to three Tor websites that had been seized by a third country.

The fact that many of the FD 1057s in the related cases that the defense has recently uncovered are substantially the same is also evidence that an NIT was deployed. *See, e.g.,* 2019/11/29 1057, attached as Ex. 23; Ex. 3 (2019/12/09 1057); 2019/12/12 1057, attached as Ex. 24; 2020/03/12 1057, attached as Ex. 25; 2020/03/23 1057, attached as Ex. 26; 2020/04/06 1057, attached as Ex. 27; 2020/10/19 1057, attached as Ex. 28. Several of these 1057s further reveal that [redacted] was not the only target website that the FBI was investigating as part of this operation, but that there were numerous target websites—about which the FBI must have exchanged information regarding with various foreign law enforcement agencies. *See*

[11] The FBI also issued later administrative subpoenas in November 2019, further demonstrating that these cases followed the same timeline, using the same form documents. *See, e.g.,* Nov. 21, 2019 Subpoena (ECF No. 335-2) (subpoena signed by Agent Donahue on Nov. 21, 2019, and issued to Cox Communications on Nov. 22, 2019, for information relating to 391 different IP addresses); Ex. 11 (Missouri Affidavit) at ¶ 33 (administrative subpoena issued to AT&T Communications, Inc., on Nov. 22, 2019); Ex. 10 (Vermont Affidavit) at ¶ 44 (administrative subpoena issued to Burlington Telecom); Ex. 13 (Maine Affidavit) at ¶ 25 (administrative subpoena issued to Charter Communications on Nov. 19, 2019).

2019/12/26 1057, attached as Ex. 29 (referring to priority target sites); 2020/07/23 1057, attached as Ex. 30 (same); 2020/08/13 1057, attached as Ex. 31 (same); 2020/08/21 1057, attached as Ex. 32 (same); 2020/08/28 1057, attached as Ex. 33 (same); 2020/09/14 1057, attached as Ex. 34 (same); 2020/09/15 1057, attached as Ex. 35 (same); 2020/09/25 1057, attached as Ex. 36 (same); 2020/10/22 1057, attached as Ex. 37 (same); 2020/08/20 1057, attached as Ex. 38.

The search warrant affidavits and complaints cited in this memorandum contain almost and/or completely identical paragraphs throughout, not just with respect to the tip or probable cause. In addition to containing identical or almost identical paragraphs, there is other evidence that form affidavits were re-used, as in Playpen, because of the volume of cases that arose from use of an NIT. For example, the North Carolina Affidavit (Ex. 9), after identifying the three residents of the subject premises, *id.* at ¶¶ 63, 65-66, 68-74, seeks a warrant to compel a different, unrelated individual (who appears to relate to a different case) to provide biometric access to devices, *compare id.* at ¶ 84 (naming unrelated person) *with id.* at ¶ 84(h) (naming three residents).

The defense's comparison of the operation to investigate [redacted] (along with other Tor websites) to Operation Pacifier as evidence that an NIT was used is not misplaced: indeed, the FBI has drawn that comparison itself. The Michigan Affidavit (Ex. 15) makes clear that the website that the FBI compared [redacted] to in this case, in Paragraph 28, and other cases, was actually Playpen, the website that was the target of Operation Pacifier, where the FBI ran the website for two weeks, during which time it deployed an NIT to force visitors to the website to reveal their true IP addresses.

| Michigan Affidavit (Ex. 15) at ¶ 24 | Affidavit (ECF No. 254-3) at ¶ 28 |
|---|---|
| "I know that it is extremely rare for an individual who takes numerous positive steps to find child pornography on a Tor hidden services website to only visit that website one time. One example of this is analysis of 'Playpen,' which was a Tor network-based hidden service dedicated to the advertisement and distribution of child pornography that operated from August 2014 until March 2015. Similar to the TARGET WEBSITE, Playpen was a highly categorized web forum with hundreds of thousands of users. . . . In February and March of 2015, the FBI seized and briefly operated the Playpen website for two weeks, using a court-authorized investigative technique to successfully identify IP addresses and other information associated with site users. The FBI's review of site data seized from the Playpen website during the operation determined that, of over 400,000 total user accounts observed on the Playpen website during its existence, less than 0.02 percent (that is, less than two hundredths of one percent) of user accounts with a registered account on the website accessed a message thread on the website only once." | "I am also aware through consultation with FBI agents that the review of detailed user data related to another Tor-network-based child pornography website found that it was exceedingly rare for a registered website user to access that website and never return. FBI review of user data from that website found that less than two hundredths of one percent of user accounts registered an account on the website, accessed a message thread on the website, and then never returned to the website and logged in to the same account." |

The similarities between this operation and Operation Pacifier are evidence that the FBI was jointly investigating [redacted] and other Tor websites as a continuation of previous efforts to take over and identify visitors to such websites. It is also evidence that law enforcement controlled [redacted] and deployed an NIT to identify visitors (which interfered with the computers of any visitors in the U.S.), contrary to what the Affidavit in this case states and implies. It is also evidence that here, like in Playpen, law enforcement have attempted to conceal information from defense teams and courts because of the controversial and possibly illegal nature of their operation.

**V. The Affidavit was additionally misleading about the meaning of the tip and whether a single visit to the target website would have been followed by additional visits.**

Recently uncovered information has further shown that Paragraph 28 of the Affidavit in this case was misleading about the meaning of the FLA tip and whether a single visit to [redacted] was likely to be associated with additional visits because it misstated the probability of users accessing the site based on materially different analysis of a prior investigation. *Compare* Michigan Affidavit (Ex. 15) at ¶ 24 *with* Affidavit (ECF No. 254-3) at ¶ 28; *see also supra* at 22.

In the Michigan Affidavit, the affiant explained that "[t]he FBI's review of site data seized from the Playpen website during the operation determined that, of over 400,000 total user accounts observed on the Playpen website during its existence, less than 0.02 percent (that is, less than two hundredths of one percent) of user accounts with a registered account on the website accessed a message thread on the website only once." *Id.* at ¶ 24. In other words, only 0.02 percent of Internet users who (1) registered an account on Playpen and (2) logged into Playpen, subsequently clicked on only one message thread; 99.98 percent of Internet users who both registered an account on Playpen and logged in to Playpen clicked on more than one message thread. *Id.* at ¶ 24. This more detailed account of the site data from Playpen appears to be the accurate recitation of that data.

In this case, Special Agent Ford (or whomever wrote the substance of the Affidavit, who was likely an agent from FBI headquarters, and not Agent Ford) sought to make the data imply something different—that logging in to the site (which there is no evidence that Mr. Sanders did), without more, statistically meant that the user must have previously been to the site and accessed illegal content in message threads (which there is also no evidence that Mr. Sanders did). Special Agent Ford claimed that the "FBI review of user data . . . found that less than two

hundredths of one percent of user accounts registered an account on the website, accessed a message thread on the website, and then never returned to the website and logged in to the same account." Affidavit (ECF No. 254-3) at ¶ 28. In other words, rather than discussing the likelihood that a registered, logged-in user would view more than one posting, Agent Ford addressed the likelihood that someone who had previously (1) registered an account, (2) logged in, and (3) accessed (*i.e.* visited) a message thread on the website would subsequently return to the website and log back in using the same credentials. *Compare* Michigan Affidavit (Ex. 15) at ¶ 24 *with* Affidavit (ECF No. 254-3) at ¶ 28.

In phrasing the statistic to imply that access to the homepage yielded a strong inference of past use of the website, that paragraph of the Affidavit incorrectly implied that the tip meant that the Internet user had taken all three steps of registering, logging in, and accessing a message thread at some prior point in time—even though there was no evidence that anyone using the Sanders family's IP address had ever done so. Paragraph 28 also incorrectly implied that the Internet user had returned to the target website more times than the single timestamp of 02:06:48 UTC on May 23, 2019 supported.

Paragraph 28, in conjunction with Paragraph 23, therefore misled the Magistrate Judge into believing that there was evidence that the Internet user either viewed child pornography on [redacted] or, in the alternative, intended to view child pornography on [redacted] when the evidence simply did not support that proposition. Accordingly, this Court should order a *Franks* hearing and suppress the evidence obtained pursuant to the illegal warrant. At a minimum, the Court should require the government to provide discovery of any review or other evidence or testimony that the government believes could support the claim made in Paragraph 28 of the Affidavit.

## VI. FLAs and the U.S. have continued to work more closely than the government previously acknowledged, undermining the government's claim that the FBI was not involved in the investigation into [redacted] that identified Mr. Sanders's IP address.

Government press releases from early March 2022 have revealed additional information about Operation H (another name for what appears to be [redacted] and/or [redacted] the operation that led to the seizure of the Sanders family's IP address and tens of thousands of other IP addresses. These documents reveal what the FBI concealed from the Magistrate Judge and what the government in this case failed to disclose to the defense and this Court. These materials reveal a higher degree of long-term cooperation between the U.S. and its foreign law enforcement partners in investigating [redacted] and other Tor sites, which is a continuation of what the FBI did in Operation Torpedo, Freedom Hosting, and Operation Pacifier. *See, e.g.,* Memorandum in Support of Renewed Motion to Suppress (ECF No. 476) at 17-19.

Contrary to what has been suggested and stated in the Affidavit, and by the government throughout the litigation of this case, the investigation into [redacted] involved not just a tip from one foreign law enforcement agency—the [redacted] to FBI, but a joint effort between the [redacted], the US, and many other countries, as part of "the largest operation of its kind" to "stop[] the spread of some of the most egregious and devasting examples of child exploitation material found on the internet to date." Operation H in Numbers, attached as Ex. 39.[12] The platform under investigation included "imagery depicting sadistic acts of sexual abuse of infants and children." 2022/03/02 Europol Press Release, attached as Ex. 40, at 1.

[12] This document was released as part of an INTERPOL press release from March 2, 2022, and is available from INTERPOL's website. *INTERPOL supports New Zealand-led international operation into online child sexual abuse material*, INTERPOL (Mar. 2, 2022), https://www.interpol.int/en/News-and-Events/News/2022/INTERPOL-supports-New-Zealand-led-international-operation-into-online-child-sexual-abuse-material (last accessed Mar. 14, 2022).

Operation H included, at minimum, the US, the UK, Canada, New Zealand, Austria, Croatia, the Czech Republic, Greece, Hungary, Slovenia, Slovakia, Spain, Europol, and INTERPOL. *See, e.g.,* Ex. 40 (2022/03/02 Europol Press Release), at 1-2; *see also* 2022/03/02 INTERPOL Press Release, attached as Ex. 41. "The international coordination of the investigative activities" among these countries and their respective law enforcement agencies "facilitated the identification of" "90,000 online accounts" and "a large number of individuals." Ex. 40 (2022/03/02 Europol Press Release) at 1. As part of this coordination, "Europol facilitated the exchange of information and coordinated the partner agencies," including by "provid[ing] analytical support by cross-checking the data and providing greater detail for the investigative intelligence packages, which were then disseminated to the national law enforcement authorities participating in this operation," which included authorities in the United States. *Id.* at 2; *see also* Affidavit in Support of Criminal Complaint (ECF No. 4) at ¶ 9 ("The FBI, in conjunction with other law enforcement entities, is investigating websites on which visitors can access and view child sexual abuse material. Through this investigation, the FBI received information that on or about May 23, 2019, an individual connected to the internet through a specific [IP] address and accessed a website that is known to law enforcement . . . "). In the UK, "[i]nformation relating to accounts believed to have been created in the [redacted] was passed to the [redacted] The [redacted] launched a high priority operation to analyse the data, before initiating its own investigations, as well as disseminating packages to law enforcement partners across the country." 2022/03/01 [redacted] Press Release, attached as Ex. 42 at 1; *see also* [redacted] Inspection Report (ECF No. 138-1) at 14 ("[redacted]

[redacted] .");[13] *see also* Regional Organised Crime Unit for the West Midlands Region Report (ECF No. 138-2) at 2.

It was at least as early as October 2019[14] that New Zealand took the lead on this operation and "brought together international law enforcement agencies including the FBI, the Australian Federal Police, the Royal Canadian Mounted Police, the National Crime Agency in the UK, Europol and INTERPOL, as well as NZ Police and New Zealand Customs Service to establish a co-ordinated approach to identifying and investigating individuals tied to these accounts. What followed was hundreds of investigations, commenced across the world." 2022/03/02 New Zealand Press Release, attached as Ex. 43, at 1; *see also* [redacted] (ECF No. 138-3) at 2) [redacted] ). The New Zealand lead for Operation H, Tim Houston, in announcing it, "commend[ed] the ongoing support of our law enforcement partners domestically and across the world" and the press release "highlight[ed] the importance of collaboration in an operation like this." Ex. 43 (2022/03/02 New Zealand Press Release) at 1-2.

[13] In another case that stemmed from the same operation as the one that identified Mr. Sanders's IP address, the tip is described as being from "a foreign law enforcement partner." Ex. 9 (North Carolina Affidavit) at ¶¶ 62, 64, 76.

[14] The third purported tip document was provided to the FBI on October 25, 2019. That report was not specific to the Sanders family's IP address and was listed as having been "[d]isseminated to: International partners in receipt of [redacted] intelligence." FLA Report (ECF No. 255-3).

## VII. At the very least, the newly-discovered material warrants additional discovery in this case.

For the reasons explained in Section I-VI, the recent disclosures demonstrate that there is a significant amount of withheld discovery material to Mr. Sanders's suppression issues that should have been produced in order for the suppression issues to have been decided on a fair and accurate record. This material should now be produced, at minimum to the Court for *in camera* inspection. Withheld material includes, e.g., the identity of the country (and agency) that infiltrated the website, the identity of the country (and agency) that deployed a technique that identified Mr. Sanders's IP address (and the circumstances of that identification); and the user history and logs from [redacted] which the FBI has now expressly admitted in the *Stauffer* Complaint (Ex. 5) as in its control and/or possession.[15]

It is further clear from the numerous substantially similar affidavits and 1057s that additional information was obtained by the FBI as a result of this operation, which was not included in any materials shared with the defense. These materials therefore contradict the government's prior claim that only three documents (ECF Nos. 255-1, 255-2, and 255-3) existed about the tip, and that the government "d[id]n't have any more exculpatory information out there about the tip that we're withholding." 2020/07/31 Tr. (ECF No. 255-1) at 26. Any additional exculpatory information about the nature of the overarching investigation should be produced.

[15] It is also clear that the U.S. was communicating back and forth about the seizure, deployment of NITs, and identification of IP addresses relating to at least three Tor websites, one of which was [redacted] For example, as part of this operation, "HSI Seattle Field Office was advised by the HSI Boston Field Office that they had been investigating individuals accessing *'dark web' sites and forums* dedicated to the sexual abuse and exploitation of children. Previously in June of 2019, a foreign law enforcement agency seized a computer server *hosting three 'dark web' sites* operating on the TOR (The Onion Router) Network." Ex. 4 (*Clark* Complaint) at ¶ 5.

## CONCLUSION

For all the reasons set forth above and in the previously filed pleadings incorporated by reference, Mr. Sanders respectfully requests that the Court grant Mr. Sanders's previously filed Motions to Compel, order a hearing pursuant to *Franks v. Delaware,* 438 U.S. 154 (1978), and suppress all evidence obtained pursuant to the invalid search warrant issued in this case because it was not supported by probable cause and was based on an affidavit containing numerous false and misleading statements and omissions.

Respectfully submitted,

/s/
Jonathan Jeffress (#42884)
Jade Chong-Smith (admitted *pro hac vice*)
KaiserDillon PLLC
1099 Fourteenth St., N.W.; 8th Floor—West
Washington, D.C. 20005
Telephone: (202) 683-6150
Facsimile: (202) 280-1034
Email: jjeffress@kaiserdillon.com
Email: jchong-smith@kaiserdillon.com

/s/
Nina J. Ginsberg (#19472)
DiMuroGinsberg, P.C.
1101 King Street, Suite 610
Alexandria, VA 22314
Telephone: (703) 684-4333
Facsimile: (703) 548-3181
Email: nginsberg@dimuro.com

/s/
H. Louis Sirkin (admitted *pro hac vice*)
Santen & Hughes
600 Vine Street, Suite 2700
Cincinnati, OH 45202
Telephone: (513) 721-4450
Facsimile: (513) 721-0109
Email: hls@santenhughes.com

*Counsel for Defendant Zackary Ellis Sanders*

**CERTIFICATE OF SERVICE**

I hereby certify that on this 14th day of March 2022, the foregoing was served electronically on the counsel of record through the US District Court for the Eastern District of Virginia Electronic Document Filing System (ECF) and the document is available on the ECF system.

*/s/ Jonathan Jeffress*
Jonathan Jeffress